Література: *1. Конституція України // Закони України. - Т.10. - К., 1997. 2. Закон України "Про інформацію" від 2.10.1992 р. // Закони України. - Т.4. - К., 1996. 3. Закон України "Про державну таємницю" від 21.01.1994р.// Закони України. - Т.7. - К., 1997. 4. Закон України "Про підприємництво" від 7.02.1991р. // Закони України. - Т.1. - К., 1996. 5. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави. КМ України , Постанова КМ № 1893 від 27.11.98// www.liga.kiev.ua 6. Закон України "Про рахункову палату" від 11.076.1996 р. // Закони України. - Т.11. - К., 1997. 7. Закон України «Про внесення змін до деяких законодавчих актів України» від 13.01.2000р.// www.liga.kiev.ua Закон України "Про інформацію з обмеженим доступом, що не становить державної таємниці": проект, підготовлений НДЦ "ТЕЗІС" НТУУ "КПІ" на замовлення Держкомсекретів України. - К., 1999. – 25 с.*

УДК 681.3

ІНФОРМАЦІЯ ЯК ЗНАРЯДДЯ ВЧИНЕННЯ ЗЛОЧИНУ ТА ЗЛОЧИНИ ПРОТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Дарія Прокоф'єва
Національний технічний університет України "КПІ"

Анотація: **стаття присвячена інформації (інформаційній зброї), яка використовується в якості знаряддя вчинення злочину.**
Summary: **this article is about the information (information weapon), which is used as an instrument of commiting a crime.**

Знаряддя вчинення злочину в теорії звичайно визначаються як предмети навколишнього світу, що використовуються злочинцями задля здійснення впливу на предмет злочинного посягання, потерпілого, інші охоронювані кримінальним законом цінності. З визнанням інформації повноправним об'єктом суспільних відносин, а також з активізацією проявів інформаційної війни [5-8], в тому числі кримінально-караних, що характеризуються здійсненням впливів на інформаційні системи різного рівня (механічні та біологічні) саме за допомогою інформації, можна дійти висновку, що знаряддям скоєння злочину може виступати також інформація, точніше – інформаційна зброя. Остання являє собою алгоритм цілеспрямованого впливу на інформаційну систему шляхом передачі такій системі інформації (або здійснення з інформацією інших запланованих дій) [5]. Тобто, інформація формує інформаційну зброю, якщо включається до цілеспрямованої програми впливу на систему-мішень, яка має бути здатною призвести до досягнення запланованих суб'єктом впливу кінцевих результатів.

Аналізуючи чинне кримінальне законодавство України [1], можна виділити наступні різновиди інформації (інформаційних впливів), що виступають в якості знаряддя вчинення злочинів:

1). Погроза (ст. ст. 86^2, 100, 123′, 127, 144, 155^5, 155^8, 176^2, 188′, 189^2, 190, 198^2, 217^2, 217^4, 228^4, 229^2, 229^{19}, 235 КК України). В усіх злочинах, які визначаються в диспозиції відповідних статей як такі, що скоюються за допомогою (шляхом) погрози (ст. ст. 86^2, 123, 127, 144, 155^5, 155^7, 188^2, 198^2, 217^2, 229^{19} КК України) або в яких діяння (обов'язкова ознака об'єктивної сторони) реалізується як погроза (ст.ст. 100, 176^2, 189^2, 190, 228^4, 235 КК України), має місце здійснення інформаційного впливу на обраного суб'єкта (мішень впливу), тобто потерпілого. Кожна інформаційна система потребує захисту від інформації, оскільки "любая поступающая на вход системы информация неизбежно меняет систему. Целенаправленное же, умышленное информационное воздействие может привести систему к необратимым изменениям и самоуничножению" [4]. Цілеспрямований умисний вплив, що призводить систему до необоротних змін або самознищення, а рівно й до зміни її поведінки в цілях, що є вигідними для особи, котра здійснює такий вплив (в контексті чинної роботи мова йде про суб'єкта злочину), однак шкідливих для самої системи, являють собою застосування інформаційної зброї з метою створення загроз інформаційній безпеці (загроз як потенційної небезпеки), а також для їх реалізації. Ці створювані та такі, що реалізуються, загрози можуть бути внутрішніми та зовнішніми, явними та прихованими. Відмітимо, що в процесі здійснення цілеспрямованого інформаційного впливу, який визнається злочинним (визначається як такий в нормах кримінального закону), створюються зовнішні загрози інформаційній безпеці, а також активізуються (провокується або каталізується їх виникнення) внутрішні загрози інформаційній безпеці. Крім того, загрози як можлива небезпека інформаційній безпеці поділяються на явні та

приховані. Явні загрози в тому значенні цього терміну, яке передбачає потенційну небезпеку, найбільш часто виражаються власне в погрозах, тобто, в залякуванні, обіцянках заподіяти шкоду (більш коректним з кримінально-правової точки зору слід визнати визначення порози як висловленого в будь-якій формі наміру завдати фізичної, матеріальної або іншої шкоди суспільним чи особистим інтересам), що чітко відображає їхній очевидний характер. Іншими словами, погрози, що виступають занряддям вчинення злочину або утворюють об′єктивну сторону злочину вцілому, стосовно безпеки інформаційних систем від інформаційних впливів виступають явними загрозами. Це, однак, не означає, що погроза як висловлений в тій чи іншій мірі намір завдати шкоди не продуціює в інформаційній системі, яка є мішенню інформаційного впливу, факторів, що відповідальні за зміну її поведінки або взагалі самознищення в інтересах того, хто здійснює вплив, тобто, внутрішніх загроз. Як видно з диспозицій статей, що передбачають відповідальність за злочини, специфіка яких розглядається (тобто, такі, що вчиняються за допомогою інформаційної зброї), погроза не є абстрактною, тобто, це висловлений (в будь-якій формі) намір завдати певній мішені інформаційного впливу певної конкретної шкоди. Це може бути висловлений намір вчинити вбивство (ст. 100 КК України), застосувати насильство (ст. 144 КК України), викрасти радіоактивні матеріали або використати їх (ст. 228^4 КК України), знищити майно або розголосити відомості, що ганьблять суб′єкта, котрий в конкретному випадку являє собою мішень інформаційного впливу, або ж погроза помстою – незалежно від передбачуваних форм її наступної реалізації (ст. 180 КК України). При цьому з точки зору застосування інформаційної зброї при скоєнні злочинів особливий інтерес становить погроза розголошення відомостей, що ганьблять суб′єкта-мішень інформаційного впливу, яка фактично має двоїстий характер: таке діяння являє собою застосування інформаційної зброї, що заключається в повідомленні інформаційній системі-мішені про те, що в перспективі проти неї буде застосовано інформаційну зброю;

2). Завідомо неправдива інформація (ст. ст. 79, 83, 87, 125, 127, 128, 129′, 143, 148^5, 148^8, 153, 153′, 155, 155′, 156^2, 156^3, 172, 177, 178, 192, 194, 198′, 206^2, 229^{18}, 243′ КК України). Застосування завідомо неправдивої інформації як різновиду інформаційної зброї становить не явну, а приховану загрозу безпеці інформаційних систем[4]. Ця теза повністю підтверджується множинністю злочинів, що скоюються за допомогою обману (серед злочинів, в яких інформація (інформаційна зброя) виступає знаряддям їх вчинення, злочини, де в якості засобу досягнення суспільно-небезпечної (шкідливої) мети використовується обман, становлять найчисельнішу групу). Разом з тим, цілі застосування такого різновиду інформаційного впливу, як обман, можуть бути різними, що, відповідно, зумовлює й віднесення статей, які передбачають склади відповідних злочинів, до різних розділів Особливої частини КК України, що відповідним чином визначає (виходячи з існуючої структури Особливої частини КК України) й об′єкти зазначених злочинів. Різними є також й способи доведення завідомо неправдивої інформації до відома потенційного потерпілого від того чи іншого злочину, віднесеного до групи, що розглядається, тобто способи подання неправдивої інформації "на вхід" інформаційній системі-мішені. Такі способи обману (доведення завідомо неправдивої інформації до відома потенційного потерпілого) перебувають в тісному взаємозв′язку з іншими елементами складів відповідних злочинів. Крім того, різним може бути ступінь так званої точності управління інформаційною системою-мішенню, що досягається шляхом обману. Низька точність управління інформаційною системою-мішенню (тобто тривалий період часу, що проходить між запланованим та дійсним досягненням мети застосування завідомо неправдивої інформації в якості знаряддя вчинення злочину) в принципі не впливає на кваліфікацію злочинів, що скоюються шляхом обману, однак значною мірою ускладнює розслідування подібних злочинів. Знання точності управління інформаційною системою, що самонавчається, має істотне значення також й для розслідування інших злочинів, що скоєні з використанням інформаційної зброї. Так само, як і інішим різновидам інформаційної зброї, завідомо неправдивій інформації, що використовується зі злочинною метою, мають бути притамані всі її (інформаційної зброї) ознаки, зокрема, суб′єктивна значимість як здатність інформаційного впливу (повідомленої в той чи інший спосіб завідомо неправдивої інформації) бути адекватно сприйнятим адресатом такого впливу, а відповідно, й призводити до запланованого винним результату.

3). Заборонена інформація та інформаційні впливи, що завідомо призводять до злочинних наслідків (ст. ст. 56′, 62, 63, 66, 99, 126, 171, 176^3, 189, 189′, 206′, 211, 211′, 229^5, 237 КК України). При цьому заборона може стосуватися здійснення різноманітних дій, предметом (об′єктом) яких є інформація певного змісту: виготовлення (створення), розповсюдження тощо, або декількох (чи всього комплексу інформаційної діяльності) дій з такою інформацією. Фактично, саме в цій групі злочинів інформаційна зброя проявляє себе як така, тобто, як зброя, що й констатує законодавець. Так само, як і для традиційної зброї, мова йде про обмеження обігу інформаційної зброї. При цьому для того різновиду інформаційної зброї, який зараз розглядається, характерно не просто обмеження участі в обізі, але й повна його заборона. Останнє наочно демонструє врахування можливостей інформаційної зброї щодо створення у випадку його застосування ситуацій підвищенної суспільної небезпеки, а відповідно, й завдання значної шкоди різноманітним суспільним відносинам. Злочини, що входять до групи, яка аналізується, утворюються власне введеням до обігу – в різних формах – інформаційної

зброї, тобто, у створенні, розповсюдженні, іншому використанні забороненої інформації, а не (як це має місце в інших групах злочинів, де інформація виступає в якості знаряддя вчинення) використання інформаційної зброї при здійсненні тих чи інших інформаційних впливів неправомірного характеру. Таким чином, вже власне введення до обігу забороненої інформації як різновиду інформаційної зброї утворює, в окремих випадках – потенційно, неправомірний інформаційний вплив. Його мішенню, що теж слід визнати специфічною рисою групи злочинів, що розглядається, як правило, виступає суспільство вцілому, тобто необмежене коло його членів та елементів. Особливо часто в якості можливих мішеней таких впливів виступають фізичні особи (їх необмежена кількість). Заборонена інформація як різновид інформаційної зброї, таким чином, не має прив′язки до конкретної інформаційної системи та особливостям її суб′єктивного сприйняття, тобто, внаслідок особливостей свого змісту (які й викликають заборону такої інформації на законодавчому рівні, та встановлення кримінальної відповідальності за її введення до обігу, тобто однозначне визначення певної інформації в якості інформаційної зброї) може з однаковою ефективністю здійснювати вплив на різноманітні їнформаційні системи, в тому числі й лише на однотипні. Все це, однак, не означає в обов′язковому порядку "загальнопоглинаючої" дії досліджуваного різновиду інформаційної зброї. Іншими словами, може існувати передача (адресування) забороненої інформації конкретній інформаційній системі (тобто, застосування проти неї інформаційної зброї), однак при цьому слід враховувати ту обставину, що з рівним успіхом зазначена інформація могла б бути застосована й до інших інформаційних систем того ж чи іншого типу. Це також свідчить про небезпеку інформаційної зброї в такій її формі, як заборонена інформація (звісно, ця назва є умовно-збиральною, і не має закріплення у відповідних правових нормах). Як вже зазначалося вище, підставою для заборони інформації є особливості її змісту, які зумовлюють здатність такої інформації негативно впливати на оточуючих (ті чи інші інформаційні системи). При цьому диференціюється наступна заборонена інформація: інформація, зміст якої становлять заклики до вчинення дій, що є небезпечними для державного ладу, територіального устрою, громадського порядка та громадської безпеки; інформація, змістом якої є відомості, що принижують честь та гідність фізичних (зокрема – посадових) осіб, висловлені в непристойній формі; інформація, зміст якої негативно впливає на громадську моральність та моральне здоров′я окремих громадян; інформація, зміст якої, після доведення його до відома конкретної інформаційної системи, здатний викликати необоротні протиправні та передбачені кримінальним законом наслідки для зазначеної системи. Остання група інформаційної зброї має специфіку порівняно з трьома попередніми. Зокрема, слід відмітити, що воне не повністю відповідає ознакам, які були описані вище, які притамані злочинам, вчинюваним за допомогою забороненої інформації як різновиду інформаційної зброї. Так, у випадку вчинення злочинів, передбачених ст. ст. 99, 171, 229^5, обов′язково присутня ознака суб′єктивної значимості інформації, що виступає знаряддям вчинення злочину. Водночас, зміст такої інформації є досить типовим, що дозволяє відмежувати її від інших знарядь здійснення інформаційних впливів як таку, що здатна викликати певний ефект (тобто, призводити до конкретного зазначеного в нормі закону протиправного результату) й заборонити такого роду інформацію до застосування (таке застосування, як правило, здійснюється за контактної взаємодії, коли винний реалізує неправомірний інформаційний вплив). При цьому про зміст інформації мова йде не як про сукупність конкретних відомостей, а про відомості певного характеру, що можуть бути сприйняті інформаційною системою-мішенню й викликати визначений законом протиправний результат. Таким чином, забороненою до застосування є будь-яка інформація, що здатна викликати: суїцид (самознищення інформаційної системи-мішені, що є об′єктом інформаційного впливу), дачу хабаря або вживання наркотиків (останні два пункти позначають також свого роду самознищувальна поведінка інформаційної системи-мішені). При цьому слід зазначити, що застосована задля досягнення зазначених протиправних результатів заборонена інформація може являти собою самостійний різновид інформаційної зброї (на відміну від інформації, що виступає знаряддям вчинення – та предметом – злочинів, передбачених ст. ст. 211, 211^1 КК України, вона набуває якостей інформаційної зброї лише у поєднанні з метою інформаційного впливу, тобто, з потенційним протиправним результатом, якого винний планує досягти в конкретній ситуації інформаційного впливу), або ж утворюватися в результаті пристосування інших видів інформаційної зброї (погроз, обману тощо) для досягнення чітко визначених цілей. В останньому випадку розглядання відповідних злочинів як таких, що скоєні за допомогою забороненої інформації зумовлене тим, що: вони не можуть бути визначені як скоювані за допомогою того чи іншого конкретного виду інформаційної зброї (лише погроз або обману, тощо); характеризуються спеціальним передбачуваним (очікуваним) результатом, досягнення якого може вимагати комплексного впливу за допомогою декількох різновидів інформаційної зброї; "забороненість" інформації викликається її здатністю призводити до певного (передбачених законом) результату, який, окрім всього іншого, не співпадає з результатом застосування того чи іншого різновиду інформаційної зброї при здійсненні самостійного, спрямованого на досягнення іншої мети, інформаційного впливу, причому не будь-яка інформаційна зброя може виступати "забороненою" інформацією, застосування якої дозволяє досягти цілей злочинів групи, що розглядається (наприклад, обман практично не може використовуватись задля скоєння злочину, передбаченого ст. 171 КК України, оскільки із застосуванням обману цей злочин буде трансформуватися на шахрайство, разом з тим, цей злочин може бути скоєний за допомогою інформації, яка не

становить ні погрози, ні обману, ні заклику до протиправної діяльності, тобто, не є забороненою об′єктивно, однак забороненість якої зумовлена особливостями мети, якої винний планує досягти із застосуванням такої інформації; причому зазначена мета завжди в тій чи іншій формі буде відображатися у змісті інформації, яка внаслідок цього стає забороненою). Таким чином, критерієм віднесення злочинів до групи, що розглядається є не певна форма інформаційної зброї, що застосовується, тобто, відповідність його уявленням про ознаки завідомо неправдивої інформації, обману, погрози тощо, а її зміст, що відображає мету запланованого неправомірного інформаційного впливу;

4). Ентропійний вплив (ст.ст. 112, 156^2, 179, 186, 187, 204, 227′, 228′ КК України). Так званий ентропійний вплив може розглядатися як від′ємний, інформаційний вплив "з позначною "мінус"". Мова йде про неповідомлення тій чи іншій інформаціній системі (яка виступатиме мішенню як впливу, так і злочинного посягання) тієї інформації, що є необхідною для її нормальної життєдіяльності (фунціонування), тобто, відсутність правомірного інформаційного впливу, не лише нешкідливого, але й необхідного для інформаційної системи, зумовлена, в свою чергу, протиправними діями винного. Подібне неповідомлення інформації (так само, як і вплив за шляхом повідомлення тієї чи іншої інформації) є цілеспрямованим і здатне викликати заплановані винним зміни поведінки інформаційної системи-мішені (тобто, інформаційної системи, якій в даному випадку інформація не повідомляється), аж до самознищення останньої. При цьому ентропійний вплив може застосовуватись й за відсутності мети змінити поведінку інформаційної системи-мішені, тобто, з метою "консервації" існуючого стану речей задля того, щоб знебезпечити суб′єкта ентропійного впливу (суб′єкта злочину) від можливих наслідків зміни поведінки інформаційної системи-адресата, до яких могло б призвести одержання останньою необхідної інформації. При цьому в окремих випадках злочини, скоювані шляхом ентропійного впливу, можуть носити й предметний характер, коли винний не лише зацікавлений в зікритті інформації з метою завдати шкоди інформаційній системі-мішені, але й коли зазначена інформація становить цінність (з тієї чи іншої причини) для винного. В окремих випадках ентропійний вплив може бути поєднаний з наданням інформаційній системі-мішені завідомо неправдивої інформації (як у випадку приховування банкрутства).

Спектр злочинів [1,2], в яких інформація (інформаційна зброя) виступає в якості знаряддя їх вчинення (зумовлюючи, в свою чергу, вчинення злочинів шляхом інформаційних впливів), є, таким чином, досить широким. Завдяки специфічним властивостям інформаційної зброї [3,4] (таким, наприклад, як вибірковий вплив та суб′єктивна значимість для мішені, що піддається впливові), а також особливостям впливу, що здійснюється за її допомогою, є можливим застосування інформаційної зброї при вчиненні злочинів, що посягають на різноманітні суспільні відносини, причому як таких, що характерізуються наявністю предмета, так і "безпредметних". В цьому інформаційна зброя подібна до традиційної, однак, сфера її застосування при вчиненні злочинів є більш широкою, ніж це має місце для традиційної зброї (не виключається і їх одночасне використання). Використання інформаційної, як і традиційної зброї, може виступати кваліфікуючою ознакою вчиненого злочину.

Водночас, не всі злочини, що скоюються із застосуванням інформаційної зброї (зокрема, з вищенаведеного переліку) можуть розглядатися як такі, що посягають на інформаційну безпеку (безпеку інформації та безпеку від інформаційних впливів). Частина з них дійсно посягає на обидва зазначені об′єкти, або ж на останній з них, в інших же посягання на безпеку від інформаційних вливів потребує додаткового розпізнавання, та, в принципі, спеціально виділяється лише умовно – з метою дослідження. Так, існує низка злочинів, що скоюються або (в якості альтернативи) можуть бути скоєні шляхом інформаційних впливів, і які на перший погляд не мають жодного стосунку до інформаційної безпеки, інформаційної війни та інформаційної сфери взагалі (хоча інформаційна сфера "пронизує" всі інші сфери суспільного життя та об′єднує їх за допомогою формування системи знань, а відповідно, злочини в інформаційній сфері та в інших сферах є взаємопов′язаними, такими, що взаємовпливають одне на інше, а в окремих випадках – взаємопереходять; взагалі, інформаційна сфера та ті суспільні відносини, що існують в її межах, становить інтерес для здійснення злочинних посягань лише в силу своєї здатності впливати на інші сфери суспільного життя, а не самі собою).

Зазначимо, що значна кількість злочинів не лише вчинюються за допомогою інформаційних впливів, але й мають інформацію (в тому числі певного виду, або вміщену на матеріальних носіях певного виду) в якості предмету. Вказані злочини посягають на безпеку інформації в аспекті її достовірності, тому не викликає сумнівів їх належність до групи інформаційних навіть в тому випадку, якщо взяти під сумнів предметний характер відповідних складів (це може мати місце, наприклад, у випадку повної підробки матеріальних носіїв інформації, коли складно – хоча й не є неможливим – вести мову про певний "об′єкт матеріального світу"- його поняття значною мірою стало умовним з визнанням інформації в якості об′єкта права власності, - впливаючи на який злочинець завдає шкоди суспільним відносинам, оскільки підробні матеріальні носії інформації не існують незалежно від злочинця й ним створюються, однак в якості предмета злочинного посягання може бути визначений клас матеріальних носіїв інформації в їх належній формі як носіїв достовірної інформації). Так, існування в обізі підробних документів (або інших матеріальних носіїв інформації) являє собою порушення (або

його реальну загрозу) безпеки суб′єктів, яким зазначені матеріальні носії інформації пред′являються, від неправдивої інформації. Порушення інформаційної безпеки внаслідок сприйняття неправдивої інформації призводить відповідно й до порушень в інших сферах суспільного життя (наприклад, майно передається особі, що не має на нього права, на підставі підробних правовстановлюючих документів). В окремих випадках, виходячи з конструкції відповідних статей в чинному КК України, в таких злочинах роль інформації є більш очевидною в якості знаряддя вчинення злочину. Це не означає, однак, що такі злочини не посягають одночасно й на безпеку інформації, тобто, не мають відповідного предмету. Злочини ж, що мають інформацію в якості предмета, становлять загрозу й для "безпеки від інформації" через використання здобутої злочинним шляхом інформації для подальшої суспільно-небезпечної діяльності (в тому числі й злочинної) в різних сферах життєдіяльності суспільства (ведення інформаційної війни [3-8]).

Водночас, як бачимо вже з вищенаведеного переліку, існують передбачені чинним КК України склади злочинів, що не завдають шкоди цілісності та (або) достовірності інформації, а рівно її законній приналежності, тобто, не можуть розглядатися як злочини проти безпеки інформації, однак інформація (інформаційні впливи) виступає знаряддям їх скоєння (наприклад, погрози або заборонена до введення в обіг інформація). Такого роду злочини являють найбільшу складність при вирішенні питання про те, чи належать вони за своєю сутністю до інформаційних злочинів або ж ні, оскільки для зазначених злочинів можливі обидва варіанти. Отже, необхідно провести відмежування інформаційних злочинів, тобто, злочинів проти інформаційної безпеки (в аспекті безпеки від інформаційних впливів) від інших злочинів, що скоюються (можуть скоюватися) за допомогою інформаційної зброї. Останні, в свою чергу, заслуговують на те, щоб стати предметом спеціального дослідження. В якості диференціюючих факторів можуть бути названі наступні:

- склад злочинів, що посягають на той чи інший аспект інформаційної безпеки (зокрема, безпеки від інформаційних впливів), "утворюється" в інформаційній сфері, тобто, має місце вже внаслідок завдання злочином шкоди власне в інформаційній сфері, незалежно від того, чи було зачеплено його (злочину) негативними наслідками інші сфери життєдіяльності суспільства;

- інформаційні впливи, метою яких є зміна поведінки суб′єктів або трансформації об′єктів в різних сферах життєдіяльності суспільства, при скоєнні інформаційних злочинів опосередковуються конкретними об′єктивними проявами в інформаційній сфері (введенням до обігу забороненої інформації, внесенням неправдивої інформації до інформаційних масивів тощо);

- прояви інформаційних впливів в інформаційній сфері є об′єктивними, тобто існують незалежно від їх суб′єктивного сприйняття, а при здійсненні сприйняття їх результатів тим чи іншим суб′єктом не залишають можливості для їх довільної оцінки (так, наприклад, офіційні документи, що пред′являються, за загальним правилом сприймаються як такі, що містять правдиву інформацію, а відповідно, заслуговують на довіру стосовно юридично значимих фактів, які такими документами посвідчуються; інформація, що вводиться до автоматизованих систем за додержання всіх необхідних умов – код, реквізити тощо – сприймається як істинна; разом з тим, погроза може бути по-різному розцінена суб′єктом, якому вона адресована, тобто, оцінюватись суб′єктом довільно, а не за заздалегідь завданою схемою).

Таким чином, керуючись зазначеними диференціюючими ознаками, можливо значно скоротити перелік злочинів, що посягають на безпеку від інформаційних впливів, відмежовуючи їх від інших злочинів, що скоюються за допомогою інформаційної зброї:

- злочини, що скоюються за допомогою завідомо неправдивої інформації (ст. ст. 79, 125, 128, 129′, 148^5, 148^8, 156^2, 156^3, 172, 177, 178, 192, 194, 198′, 206^2, 229^{18}, 243 КК України);

- злочини, що скоюються за допомогою погроз, виходячи з вищенаведених дифференціюючих ознак, будуть випадати з системи інформаційних злочинів, оскільки наслідки їх скоєння не мають об′єктивних проявів, а власне злочини не можуть вважатися закінченими після самого лише впливу на інформаційну сферу. Водночас, такого роду інформаційні впливи для визнання їх злочинними підлягають відповідній суб′єктивній оцінці. Тому представляється більш доступним для розуміння та практичного застосування тлумачення відповідних складів злочинів не як інформаційних (навіть у випадку, коли склад злочину в аспекті об′єктивної сторони повністю утворений власне погрозою, тобто, специфічним інформаційним впливом), а таких, що посягають на інші об′єкти (тобто, не на інформаційну безпеку). Крім того, таке їх тлумачення – як "традиційних" злочинів, що скоюються за допомогою інформаційної зброї – потенційно викличе меньше заперечень від представників традиційних поглядів на інформацію та на структуру Особливої частини КК. Водночас, окремі злочини, наприклад, передбачені ст. 100 або 86^2 КК України, не просто вчиняються з використанням інформаційної зброї – власне вже інформаційний вплив утворює злочинне діяння, тобто, обов′язкову ознаку об′єктивної сторони злочину, а крім того (особливо це має місце стосовно злочину, передбаченого ст. 100 КК України), не повною мірою вкладаються в рамки об′єктивної типології, яка лежить в основі розмежування злочинів за групами в Особливій частині КК України;

- заборонена інформація та інформаційні впливи, що завідомо призводять до злочинних наслідків (ст. ст. 56′, 62, 63, 66, 126, 206′, 211, 211′ КК України);

- ентропійний вплив (ст.ст. 112, 156^2, 179, 186, 187, 204, 227′, 228′ КК України).

Наведений перелік дозволяє скласти уявлення про систему злочинів проти безпеки від інформаційних впливів (в тому числі й ентропійних, які являють собою неповідомлення адресатові необхідної йому інформації, зокрема й коли надання такої інформації є обов′язком винного). В сукупності зі злочинами проти безпеки інформації (при цьому низка злочинів є такими, що перетинаються) чинний перелік складає систему злочинів проти інформаційної безпеки, існування якої гіпотетично припускається, зміст якої (але не форма) закріплений в чинному кримінальному законодавстві. На даному етапі відокремлювана умовно, ця система дає змогу дійти висновків про перспективи розвитку кримінального права та законодавства у відповідній сфері в умовах розвитку інформаційного суспільства. Зокрема, мова йде про доцільність створення окремої глави в структурі Особливої частини КК за принципом специфіки об′єкта, присвяченої наведенню складів злочинів, що посягають на інформаційну безпеку, а також встановлення за їх скоєння кримінальної відповідальності. В умовах інформаційного суспільства зміст такої глави КК не може обмежуватись лише складами злочинів з наведеного вище переліку чи його модифікаціях (оскільки склади окремих злочинів з урахуванням їх інформаційного характеру у диспозиції відповідних статей в існуючому варіанті сформульовані не досить коректно, що, однак, в більшості випадків може бути виправлено підвищенням ступеня узагальнення у формулюванні). Тому обов′язковою умовою підвищення ефективності кримінально-правового захисту інформаційної безпеки є розробка концепції (на основі даних про існуючі відповідно до чинного КК України злочини проти інформаційної безпеки) вдосконалення кримінального законодавства у зв′язку з переоцінкою значення інформації як предмету злочинних посягань (й, відповідно, інформаційної безпеки як об′єкту злочину) та можливостей інформаційної зброї в умовах інформаційного суспільства.

Литература: *1. Кримінальний кодекс України. // www.liga.kiev.ua; 2. УК Российской Федерации,от 13.06.1996г. № 63-ФЗ// Собрание законодательства РФ.1996.№25. 3. Грешевников А. Информационная война. – М.: Русскій міръ, Рыбинск: Рыбынское подворье, 1999. 4. Расторгуев С.П. Информационная война. - М.: Радио и связь, 1998. 5. Горбенко І.Д., Долгов В.І., Гріненко Т.О. Інформаційна війна – сутність, методи та засоби ведення// Правове, нормативне та метрологічне забезпеченя системи захисту інформації в Україні: Матеріали ювілейної науково-технічної конференції. - К., 1998. С.36-40. 6. Завадский И.И. Информационная война - что это такое ? // Конфидент. 1996. № 4. С.13-20. 7. Кузнецов П.А. Информационная война и бизнес // Конфидент. 1996.№ 4. С.21-23. 8.Черешкин Д.С., Смолян Г.Л., Цыгичко В.Н .Реалии информационной войны// Конфидент. 1996. №4. С.9-12.*

УДК 681.3 : 34

ОХРАНА СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ УКРАИНЫ, ПРИ ОСУЩЕСТВЛЕНИИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА

Виталий Шаповаленко, Андрей Малахов, Олег Зайцев
Служба безопасности Украины

Аннатация: **Рассмотрен порядок передачи иностранным государствам секретной информации и основные разделы Соглашения о взаимной охране государственных секретов.**
*Summary:***Procedure of assignation of the secret information to other foreign states and the main parts of the agreement about mutual protection of the state secrets are presented in this article.**
Ключевие слова: **международное сотрудничество, охрана государственной тайны, Служба Безопасности Украины, экспертный контроль.**

Вопросы охраны сведений, составляющих государственную тайну Украины (секретной информации), при осуществлении международного сотрудничества регламентируются следующими нормативно-правовыми актами:

- Законом Украины «О государственной тайне»;
- Указом Президента Украины «О порядке подготовки международных договоров Украины о взаимной охране государственной тайны»;